

LISA Conference 2008

WTFM: Documentation and the System Administrator

Examples



Janice Gelb
Senior Developmental Editor
Sun Microsystems, Inc.

Procedure Guidelines

Example 1

Awkward

User Queries

When the system is introduced, it may cause a slight increase in Service Desk calls as every Internet user is potentially impacted. Measures taken to offset calls have included:

- Testing of Restricted list Internet Sites
- Splash screen developed for user information
- Online form requests and automated service desk creation

User issues will mainly be contained to three categories.

- A site they need access to has been blocked.
- A site is currently allowed that the business may want blocked.
- A file is being blocked as the system believes it is infected or contains malicious software.

OVSD issues raised should be allocated to the INTERNET for Jetsons Application and Configuration Item. White and black listing issues as discussed below should be allocated to the CORPORATE SECURITY team initially for approval and then the Service Desk for White List activation and OPS UNIX teams for blacklist activation.

Calls received in regard to malicious software, such as files required that have been blocked due to virus and require resolution, should be allocated to the OPS-WINDOWS team as per normal virus activity.

Queries will mainly be in regard to access to Internet sites that are blocked. The users will receive this message when this occurs.

Blocked by Web Gateway

Your access to the URL

`http://(insert url here)/`
was blocked because the site is blacklisted.

Should you have a legitimate business need to access the site, contact the Jetsons IT Service Desk on 1-800-555-1212, option 4 and an exception will be arranged or [click here](#) to fill in a request for exclusion.

Thanks
Corporate IT Security

The URL redirected to is <http://csit1.jetsons.com/servicedesk/itforms/restrictedSites.php>.

A variant of this message will be displayed when a user attempts to download a file that contains a virus or some other form of malware on a non-blacklisted site. The error clearly indicates "because the file contains a virus" rather than "because the site is blacklisted". This message will occur if users attempt to access sites which are in blocked categories. A list of blocked categories can be found on the Intranet FAQ. A process has been established for users to request a site to be white listed.

When the users click the link on the webpage, they will be presented with a form which they complete with the business justification for white listing the site. The URL of the site is automatically captured. When submitted, the form details are emailed by the itsecurity_ovsd@jetsons.com mailbox to OpenView Service Desk and a request for service ticket is created and automatically assigned to CORPORATE SECURITY to action.

Better

Blocked Site Process

To assist users and reduce support calls, the blocked sites effort includes:

- Testing of restricted Internet sites
- Splash screen providing user information
- Online form to request delisting a site that produces an automatic service ticket
- List of the blocked categories on the Intranet FAQ

Users are likely to experience the following issues:

- A blocked site to which they need access
- A permitted site that the business wants blocked
- A file blocked because the system evaluates that it is infected or contains malicious software.

When a user accesses a site in a blocked category:

1. The following message appears. (The text changes slightly depending on whether the site is blacklisted or has been evaluated as containing malware or a potential virus.)

Your access to the URL <URL> was blocked because the site is blacklisted. Should you have a legitimate business need to access the site, call the IT Service Desk on 1-800-555-1212, and choose option 4 to arrange for an exception. You can also fill out an [online request](#) for an exclusion.
2. If users wants to request that the site or file be re-evaluated, they submit the online request form, which is located at <http://csit1.jetsons.com/servicedesk/itforms/restrictedSites.php>.

The submission of the form triggers the following actions:

- a. The URL of the site is automatically captured.
- b. The form is sent to the itsecurity_ovsd@jetsons.com mailbox.
- c. The mail program forwards the form to the Service Desk.
- d. A Request for Service Ticket is created and allocated to the Corporate Security team.

The ticket Area is "Jetsons Application and Configuration" and the Category is "Internet."

- e. The Corporate Security team evaluates the request.
 - Blacklisted sites are sent to the OPS UNIX teams.
 - Sites approved for access are sent to the Service Desk for activation.
 - Required files blocked due to a suspicion of a virus or malware are sent to the OPS Windows team.

Example 2

Awkward

Overview of how to implement Standard or Non Standard servers

There are two processes for implementing / handing over a server from procurement to operational deployment. The process depends on whether the server is a 'Standard' or a 'Non Standard' server.

1: The Standard server Handover process

Definition of a standard server:

1. Is not part of an enterprise application or system (ie its a File / Print server)
2. Can be completely built without requiring access to the server room or leaving the site.

Process

1. Reserve a server name via the Change office
2. Complete the CMDB_upload.xls
3. Complete the Physical Host Design.doc

Note: Each team completes their relevant colour coded cells

4. Create a '**Minor**' Change record to install the server. Use the '**Server Install**'
5. Change template and attach the completed 'CMDB upload' and 'Physical Host Design' form to the Change Record.

Note: The team leader can not approve the Change until those documents are completed.

2: The Non-Standard server Handover process

Definition of a Non-Standard server:

- It is part of an enterprise application or system
- It requires access to the server room or to leave the site in order to be built

Process

1. Complete a **High level design** document.
This is signed off by a Team Leader from Operations and Tech Dev
2. Complete a **Detailed Design** document.
This is signed off by a Team Leader from Operations and Tech Dev
3. **Reserve a server name** via the Change office
4. Complete '**Section 1**' of the **Physical Host Design** form.
5. Create a '**Minor**' **Change** record to install the server into the build room / off site Attach the Configuration and Physical Host Design form to the Change Record
Note: The team leader can not approve the Change until those documents are completed.
6. Complete '**Section 2**' (and relevant appendix) of the **Physical Host Design** form
Note: Each team completes their relevant color coded cells
7. Complete the **CMDB Upload spreadsheet**
8. Complete the **Support Handover** document. Attach the High level and Detailed design doc if required.
This is signed off by a Team Leader from Operations, Tech Dev and Service Desk. Email the document to George Jetson, for Document Management.

9. **Train** Operations and Service Desk Team Leaders Create a '**Medium**' **Change** record to activate the application / system into Production
10. Attach the completed Physical Host Design form to the Change Record.
11. Attach the 'Server CI upload' spreadsheet to the Change record

Note: During the project ensure that the Support Handover plan is to be filled in as an **ongoing** basis and is not left to the end of the project.

For a detailed explanation of the each step in the either process view the 'WOW-Implement Non Standard Server_V1.pdf' or 'WOW-Implement Standard Server_V1.pdf'

All the forms and documents can be found on the Project management intranet:

<http://intranet.jetsons.com/Corporate IT/Project Office/Project Office Library/index.jsp>

Better

Implementing and Handing Over Standard and Non-Standard Servers

This section provides an overview describing how to hand over a server from procurement to operational deployment. For a more detailed explanation of these processes, see WOW-Implement Non Standard Server_V1.pdf and WOW-Implement Non Standard Server_V1.pdf. These documents and all forms mentioned in this overview are available at

http://intranet.jetsons.com/Corporate_IT/Project_Office/Project_Office_Library/index.jsp.

How you implement and hand over a server from procurement to operational deployment depends on whether the server is non-standard or standard.

- A *non-standard* server is part of an enterprise application or system. Building it requires access to the server room or the data center.
- A *standard* server is not part of an enterprise application or system (for example, a file or print server). You can build it on site without requiring access to the server room.

To Hand Over a Standard Server

1. Reserve a server name through the Change office.
2. Complete the CMDb_upload.xls spreadsheet.
3. Complete the Physical Host Design.doc form.

Note: Each team should fill in the color-coded cells relevant to their area.

4. Create a Minor Change Record to install the server.
 - a. Use the Server Install Change template.
 - b. Attach the completed CMDb Upload and Physical Host Design form to the Change Record.

Note: The team leader cannot approve the Change until those documents are completed.

To Hand Over a Non-Standard Server

1. Complete a High Level Design document and have it signed off by a Team Leader from Operations and Tech Dev.
2. Complete a Detailed Design document and have it signed off by a Team Leader from Operations and Tech Dev.
3. Reserve a server name through the Change office.
4. Complete Section 1 of the Physical Host Design form.
5. Create a Minor Change Record to install the server into the build room or offsite.
6. Attach the Configuration and Physical Host Design form to the Change Record.

Note: The team leader cannot approve the Change until those documents are completed.

7. Complete Section 2 and the relevant appendix of the Physical Host Design form.

Note: Each team should fill in the color-coded cells relevant to their area.

8. Complete the CMDb Upload spreadsheet

9. Complete the Support Handover document.
 - a. Attach the High level and Detailed design document if required.
 - b. Get sign-off of the High Level and Detailed design document by a Team Leader from Operations, Tech Dev and Service Desk.
 - c. Email the document to the Document Management liaison to Operations.
10. Train Operations and Service Desk team leaders.
11. Create a Medium Change Record to activate the application or system into Production.
 - a. Attach the completed Physical Host Design form to the Change Record.
 - b. Attach the 'Server CI upload' spreadsheet to the Change record

Tip: During the project, periodically update the Support Handover plan on an ongoing basis and do not leave gathering the necessary information to the end of the project.

Example 3

Awkward

Configure the Web Server

The following instructions are for the Apache Web server, and should be adapted if you plan on using another server.

1. If you are using the Apache server, you may use the validator under mod_perl2. This should happen automatically if you are using the httpd.conf snippet distributed with the validator or something similar, and your Apache server has mod_perl2 installed and enabled. Using mod_perl2 will bring important performance benefits, but has not been tested extensively. If you are successfully running the validator under mod_perl, or run into issues doing so, contact us.

Also worth enabling within Apache is mod_expires, which will allow caching of the validator's static documents, stylesheets, and images.

2. Edit the configuration of your Web server to refer to the specific configuration file for the validator.

This can be done by inserting the contents of the httpd/conf/httpd.conf file (from where you unpacked the validator's tarball above) in your httpd.conf, or by copying the file somewhere and including it like:

```
Include /where/you/copied/it/httpd.conf
```

Then, start editing the validator specific part.

3. You may want to set up a "virtual server" for the service. This can be done by adding something similar to the following:

```
<VirtualHost 127.0.0.1>
    DocumentRoot [validatorpath]/htdocs/
    ServerName validator.example.org
</VirtualHost>
```

AND/OR you may want to have the service at a specific location on your Web server, which can be configured as follows:

```
Alias /validator/ [validatorpath]/htdocs/
```

4. Finish editing this HTTP server configuration file, adapting all the directory references to reflect the paths used in your installation.
5. Now restart the Web server to activate the updated configuration.

For Apache this is done by typing into a shell, as System Administrator: `apachectl graceful` (or, for older versions of Apache `apachectl configtest` then `apachectl restart`)

Better

To Configure an Apache Web Server

If you are using a different web server, substitute the relevant commands.

1. If you have mod_perl2 installed and are using the httpd.conf distributed with the validator, use the validator under mod_perl2.

If you are successfully running the validator under mod_perl, or run into issues doing so, contact IT Support.

2. Enable mod_expires to enable caching of the validator's static documents, stylesheets, and images.
3. Edit the configuration of your Web server to refer to the specific configuration file for the validator by inserting the contents of the httpd/conf/httpd.conf file in your httpd.conf file.

You can also copy the file and include it by typing the following command:

Include *directory*/httpd.conf

4. In the httpd.conf file, establish the location for the service.
 - To set up a virtual server for the service, add information similar to the following:
<VirtualHost 127.0.0.1>
 DocumentRoot *validator-path*/htdocs/
 ServerName validator.example.org
 </VirtualHost>
 - To have the service at a specific location on your Web server, add information similar to the following:
 Alias /*validator*/ *validator-path*/htdocs/

1. Adapt all the directory references in httpd.conf to reflect the paths used in your installation.
2. Restart the Web server to activate the updated configuration by typing the following command as system administrator:

apachectl graceful

For older versions of Apache, use the following commands:

apachectl configtest

apachectl restart

Example 4

Awkward

Equipment Relocation Policy

Prior to the relocation or movement of any microcomputer or terminal attached to a local area network or host computer system managed by Information Technology Services, the department initiating the relocation/movement must notify Information Technology Services of its intent by submitting the Request for Support System.

Prior to the relocation or movement of any computing equipment (regardless of whether it is attached to a network or host system or is a stand alone unit), wherein Physical Facilities has been enlisted to perform the actual relocation/movement, the equipment must be certified as prepared for relocation/movement.

Certification of equipment attached to systems managed by Information Technology Services must be made by Information Technology Services. Information Technology Services will, at the request of the department initiating the relocation/movement, prepare and certify any equipment that is not attached to a network or host system. If the department chooses to prepare and certify its own equipment, it is the department's responsibility to make such certification known to Physical Facilities.

Physical Facilities will not relocate or move computing equipment that has not been certified. Information Technology Services does not perform the actual relocation or movement.

Better

Equipment Relocation Policy

Before the relocation or movement of any microcomputer or terminal attached to a local area network or host computer system managed by Information Technology Services, the department initiating the relocation or movement must perform the following actions:

1. Notify Information Technology Services of its intent by submitting the Request for Support System.
2. Make sure that any computing equipment (regardless of whether it is attached to a network or host system or is a standalone unit) to be relocated or moved by Physical Services is certified as prepared for relocation or movement
 - Equipment attached to systems managed by Information Technology Services must be certified by Information Technology Services.
 - Equipment that is not attached to a network or host system can be certified by Information Technology Services at the request of the department initiating the relocation or move, or the department can prepare and certify its own equipment. Departments choosing to prepare and certify their own equipment must make such certification known to Physical Facilities.

Physical Services will not relocate or move computing equipment that has not been certified.

Example 5

Awkward

Fixing a Commit (Log) Message

Oops, you just made a typo in your commit message. What do you do? First, figure out the revision number. You could look in the email that is sent, or do an "svn log" on a file that changed. Pretend the revision number is 6311. Put a new commit message in a file called *msg.6311*. Now run this command, but edit the underlined part:

```
svnadmin --bypass-hooks setlog /p/vdt/workspace/svn -r 6311 msg.6311
```

Note that the hooks will not be run: this means that the RT ticket (if any) will not be updated, and no email will be sent about your change.

Better

To Correct a Commit Message

1. Determine the revision number by looking in the email message sent by *[what or whom?]* or issuing the following command for a file that changed:

```
# svn log filename
```

2. Create a new file named *msg.rev-no*, where *rev-no* is the revision number.
3. Substitute the message by issuing the following command.

```
svnadmin --bypass-hooks setlog /p/vdt/workspace/svn -r rev-no msg.rev-no
```

Because hooks are not run, the RT ticket (if any) will not be updated and no email is sent about the change.

Example 6

Awkward

3. If you are about to perform a merge, create a tag. If you just created a tag for a release, use that tag. If you did not do a release, and have not yet created a tag, do so now (look at the section above on tagging for help naming the tag). This helps keep track of where the last merge point was on a given branch. The tag will likely look something like:

```
svn copy $SVN/vdt/branches/vdt-1.8.1-dcache $SVN/vdt/tags/vdt-1.8.1-dcache-merge1
```

Better

3. Before you create a merge, create a tag.

Tags help keep track of where the last merge point was on a given branch.

- If you just created a tag for a release, use that tag.
- If you have not yet created a tag, create one now.

For more information, see “Creating a Tag.”

The tag should resemble the following example:

```
svn copy $SVN/vdt/branches/vdt-1.8.1-dcache $SVN/vdt/tags/vdt-1.8.1-dcache-merge1
```

List Guidelines

Example 1

Awkward

Services may need to move between hosts, e.g. because of hardware failures or updates to more capable hosts. To facilitate this

- use hostname aliases (DNS cnames) when referencing a host that provides a specific service. Some examples are:
 - `http://www.math` is the math WWW server.
 - `mail.math` is the preferred SMTP/POP/IMAP server for the research environment.
- keep the DNS TTL low (an hour) for the aliases so that unforeseen switching to different hosts can be done in a reasonable time. It's not clear what the best balance is between keeping the TTL low to allow quick switching between hosts, and keeping the TTL high enough to avoid excess DNS queries. We chose one hour to begin with, as we can't imagine anything higher being useful. That doesn't preclude lowering it later. Unfortunately we've no means to compare the effects of changing the TTL.

Better

Services sometimes need to move between hosts, for example, because of hardware failures or upgrades.

To facilitate service transfers:

- Use hostname aliases (DNS cnames) when referencing a host that provides a specific service. For example:
 - `http://www.math` is the math Internet server
 - `mail.math` is the preferred SMTP/POP/IMAP server for the research environment
- Keep the DNS time-to-live (TTL) value low (for example, an hour) so unforeseen switches to different hosts can be done in a reasonable time.

Although this value should be set low enough to allow quick switching between hosts, setting it too low might cause excessive DNS queries. You can change this value at a later time. Our experience is that one hour is a reasonable time limit.

Example 2

Awkward

The following best practices apply to files which reside on Central File Services network drives.

- Keep the folder and file names short and use only valid characters.
 - There is a 255 maximum character limit. The folder and file name, including all parent and sub folders, must be within this 255 character limit.
 - Spaces, Letters, and Numbers are always allowed in folder and file names, but some symbols, including the following are not allowed:

\ / : * ? " < > |

An error message will appear if trying to use these characters in a name.

- A thoughtful choice of folder names can help organize work and save a lot of time hunting for the right document. Files can be grouped by task, type, author, or to whom they are going. Files having to do with classes could be put into a single folder called "Class" or "Lessons". Or you could group files by date, such as "December 2008." This leaves a wide variety of choices and still allows you to keep file names short.

Better

When organizing files on Central File Services network drives:

- Keep folder and file names short and use only valid characters.
 - Folders and file names cannot be longer than 255 characters, including all parent folders and subfolders.
 - Spaces, letters, and numbers are allowed in folder and file names. However, do not include the following symbols: \ / : * ? " < > |
- Develop a naming system to help organize work and avoid having to hunt for documents.

For example, you could group files by task, type, author, or purpose. Files having to do with classes could be put into a single folder called Class or Lessons. Or, you could group files by date, for example, December08.

Example 3

Awkward

University of Zim Policies and Standards

- <http://www.uz.edu/it/policies> - Links to many UZ policies including the *Acceptable Use Policy*, *Data Protection and Security Policy* and *World Wide Web Pages Policy*
- <http://www.hipaa.uz.edu> - Links to UZ HIPAA-standards for security. This site can only be read on campus.

Security Code Standards

1. Contingency Planning Standard
 2. Information System Account Management Standard
 3. Information Systems and Network Access Standard
 4. Internet and Email Use Standard
 5. Media Reallocation and Disposal Standard
 6. Risk Analysis and Management of EPHI Standard
 7. Security Incident Response Standard
- http://students.uz.edu/academics/student_records – *Student Records Policy* detailing what information regarding a student can be released without their permission.

Better

University of Zim Policies and Standards

The main sites for UZ policies are:

- <http://www.uz.edu/it/policies> – Provides links to many UZ policies, including the *Acceptable Use Policy*, *Data Protection and Security Policy* and *World Wide Web Pages Policy*
- <http://www.hipaa.uz.edu> - This site can be accessed only on campus. It provides links to UZ HIPAA (Health Insurance Portability and Accountability Act) standards for security. The security code standards are as follows:
 - Contingency Planning
 - Information System Account Management
 - Information Systems and Network Access
 - Internet and Email Use
 - Media Reallocation and Disposal Standard
 - Risk Analysis and Management of EPHI (Electronic Protected Health Information)
 - Security Incident Response
- http://students.uz.edu/academics/student_records – The *Student Records Policy* describes what information regarding a student can be released without their permission.

Example 4

Awkward

Data custodians must:

- Designate appropriate individuals with system administration responsibilities, ensuring that their role in securing the system is defined in their job description, and that they are trained in administration and security of the system.
- Ensure adherence to UZ guidelines and procedures for protecting data as found in [IT Security Practices](#).
- Ensure compliance with all stipulations of this and other UZ policies and other legal and regulatory requirements including those related to dissemination of data (UZ's [Information Disclosure and Confidentiality Policy](#)) and disposal of computer equipment and systems (UZ's [Equipment Accounting](#) standards, and [Secure Disposal of Media Containing Sensitive Information](#)).
- Ensure that risk assessments are performed (including disaster recovery plans, backup and contingency plans) as required by HIPAA for all PHI. Risk assessment is recommended for all other sensitive or mission critical data.
- Ensure that documentation of data resources created, used, or stored within their area of control is maintained.
- Ensure that systems containing sensitive information are physically secured from unauthorized access.
- Ensure that the department/unit follows procedures to mitigate all identified compromises or identified data security threats.
- Ensure that actual or suspected data security breaches, especially when involving sensitive data, are reported to the Data Security Office immediately and that any recommended corrective action is implemented.

Better

Data custodians are responsible for ensuring compliance in the following areas:

- Designation of appropriate individuals with system administration responsibilities, ensuring that their role in securing the system is defined in their job description, and that they are trained in administration and security of the system.
- Adherence to UZ guidelines and procedures for protecting data as found in [IT Security Practices](#).
- Compliance with all stipulations of this and other UZ policies and other legal and regulatory requirements including those related to dissemination of data (UZ's [Information Disclosure and Confidentiality Policy](#)) and disposal of computer equipment and systems (UZ's [Equipment Accounting](#) standards, and [Secure Disposal of Media Containing Sensitive Information](#)).
- Performance of risk assessments (including disaster recovery plans, backup and contingency plans) as required by HIPAA for all PHI. Risk assessment is recommended for all other sensitive or mission critical data.
- Maintenance of documentation of data resources created, used, or stored within their area of control.
- Physically securing from unauthorized access all systems containing sensitive information.
- Following procedures to mitigate all identified compromises or identified data security threats.
- Reporting actual or suspected data security breaches, especially when involving sensitive data, to the Data Security Office immediately and implementing any recommended corrective action.

Procedures and Lists Example

Awkward

HelpDesk Ticket Handling Process

- Routed correctly? Use SPDB if required to check to see if the ticket has been routed to the correct group. To access SPDB go to http://apps.main/internal/rcdb/spdb/main.cgi?nav_path=-2_2_0-33
- On taking ownership of a ticket please check the notes to see if any child tickets have been logged. If there has been a child ticket logged, add a note to the ticket saying that you are now the ITOPS contact for the ticket.
- Related Remedy or HelpDesk ticket? If a related Remedy ticket exists the ticket needs to be assigned to the same person who has the Remedy ticket, to avoid duplication of work.
- Whilst working the issue in HelpDesk follow the ITOPS Call Ticket Handling procedures at:
<http://ITmain.jetsons.com/gm/document-1.9.829482>
 - Always update the ticket at each step in the process and as per the ticket handling procedures as above.
 - If the incident can be resolved by another partner transfer the ticket. If you are not sure where to transfer the ticket use SPDB.
 - If multiple actions are required and some of these need to be done by our partners raise a child HelpDesk ticket to our partner and add a note to the ticket indicating the ticket number for any tickets raised.
- Update ticket per standard protocol
 - Ensure the incident is updated on a regular basis the standard is: Interval P 1 – 1 hr Interval P 2 & 3 – keep audit & update at least every 7 days
 - NOTE updates to the ticket are not automatically sending e-mails to customer! Make sure to select customer name (when adding a note to the ticket) – this will send e-mail to the customer.
- If this is a user submitted issue :
 - You should attempt to reach the customer at least 3 times within the targeted closure time:
 - Priority Contact Policy: P1 3 contacts over 8 hours: P2 3 contacts over 48 hours: P3 3 contacts over 64 hours
- Create stub if no JetFix article exists.
 - When you have information that could be useful in JetFix you need to update the JetFix article to ensure the next person is able to fix the problem.
- Close ticket
 - On close screen if you do not have a JetFix id or bug id field present change the Task type on the ticket to “ITOPS Production Operations”.
 - Enter the bug id listed in the sunsolve article if one is listed in the JetFix article. This is will be used to prioritize Root Cause Corrective Actions (RCCA).
 - Every ticket in HelpDesk must have a JetFix ID. If there is a valid reason for not having a JetFix id enter “na” in the JetFix id field. If there should have been a JetFix article but none could be found enter “0”.

Better

HelpDesk Ticket Handling Process

If you take ownership of a ticket, follow the ITOPS Call Ticket Handling procedures at <http://ITmain.jetsons.com/gm/document-1.9.829482>.

1. Determine whether the ticket has been routed correctly by using SPDB at http://apps.main/internal/rcdb/spdb/main.cgi?nav_path=-2_2_0-33.
2. Determine who should be handling the ticket.
 - If a related Remedy ticket exists, assign the HelpDesk ticket to the person handling the Remedy ticket.
 - If no related Remedy ticket exists, take ownership of the ticket.
1. Once you have ownership of the ticket, check the notes to determine whether any child tickets have been logged. If so, add a note to the child ticket indicating that you are now the ITOPS contact for the ticket.
2. Determine whether partner involvement is appropriate.
 - If a partner can resolve the incident, transfer the ticket. If you are not sure where to transfer the ticket, use SPDB.
 - If the solution requires multiple actions and some of those actions need to be done by partners, raise a child HelpDesk ticket to the partner and add a note to the ticket indicating the ticket number for any tickets raised.
1. Update the ticket at each stage in the process and at the recommended intervals in the standard protocol.
 - For P1 tickets, update every hour.
 - For P2 and P3 tickets, update at least every seven days and keep an audit.

NOTE: Updates to the ticket are not automatically sent to the customer. To copy the customer on the update, select the customer name when adding a note to the ticket.

1. For user-submitted issues, attempt to reach the customer at least three times within the targeted closure time:
 - P1 tickets: 8 hours
 - P2 tickets: 48 hours
 - P3 tickets: 64 hours
1. If your solution to this problem could be useful to customers using the JetFix knowledgebase, update the related article or create one if no JetFix article exists.
2. When solved, close the ticket by *[how - select Close in an interface somewhere?]*

NOTE: Do not close the ticket until all child HelpDesk tickets are closed.

- a. Provide the bug ID.
 - If the Close window does not show a JetFix ID or Bug ID field, set the Task type to ITOPS Production Operation.
 - If a Bug ID field appears, provide the bug ID listed in the relevant JetFix article.
- a. Provide the JetFix ID required for most HelpDesk tickets.
 - If you could not find a related JetFix article, type 0 in the JetFix ID field.
 - If the ticket does not require a JetFix ID, type NA in the JetFix ID field.

Table Guidelines

Example 1

Awkward

Reference Documents

Title	Organisation	Author	Version
NetBackup Administration Guide	VERITAS Software	VERITAS	5.1
NetBackup Media Manager Administration Guide	VERITAS Software	VERITAS	5.1
NetBackup GDM Administration Guide	VERITAS Software	VERITAS	5.1
NetBackup DB2 Agent Administration Guide	VERITAS Software	VERITAS	5.1
NetBackup SQL Agent Administration Guide	VERITAS Software	VERITAS	5.1
NetBackup Sybase Agent Administration Guide	VERITAS Software	VERITAS	5.1
NetBackup Lotus Notes Agent Administration Guide	VERITAS Software	VERITAS	5.1
NetBackup Vault Administration Guide	VERITAS Software	VERITAS	5.1
Command Central Service Administration Guide	VERITAS Software	VERITAS	5.1

Better

Reference Documents

Reference documents related to this product include the following documents from VERITAS Software for version 5.1:

- *NetBackup Administration Guide*
- *NetBackup Media Manager Administration Guide'*
- *NetBackup GDM Administration Guide*
- *NetBackup DB2 Agent Administration Guide*
- *NetBackup SQL Agent Administration Guide*
- *NetBackup Sybase Agent Administration Guide*
- *NetBackup Lotus Notes Agent Administration Guide*
- *NetBackup Vault Administration Guide*
- *Command Central Service Administration Guide*

Example 2

Awkward

Help Desk tickets will be assigned to the following groups:

- If the violation is copyright infringement - it is assigned to the Network group.
- If the violation is anti-virus - it is assigned to the Network group.
- If the violation is a security issue - it is assigned to the Cybercrime & Security group.
- If the violation is an appropriate use violation, such as pornography - it is assigned to the Cybercrime & Security group.
- If the violation is Groupwise email related, i.e. sending spam or inappropriate use of email - it is assigned to the Groupwise Systems group.
- If the violation is MIX (student) and other non-Groupwise email related - it is assigned to the Systems group.

Better

Help Desk ticket assignments are listed in the following table.

Violation	Group Assignment
Copyright infringement	Network
Anti-virus	Network
Security	Cybercrime & Security
Inappropriate use (for example, pornography)	Cybercrime & Security
Groupwise email-related (for example, sending spam or other inappropriate use of email)	Groupwise Systems
MIX (student) or other non-Groupwise email-related	Systems

Example 3

Awkward

Storage Encryption

	Unclassified	Confidential	Confidential: Internal Only	Confidential: Restricted	Personally Identifiable Information (PII)
Windows XP	FREE CompuSec is recommended	FREE CompuSec	FREE CompuSec	FREE CompuSec	FREE CompuSec
Windows Vista Ultimate	BitLocker is recommended	BitLocker	BitLocker	BitLocker	BitLocker
Windows Vista (all other versions)	FREE CompuSec is recommended	FREE CompuSec	FREE CompuSec	FREE CompuSec	FREE CompuSec
Mac OS X	FileVault is recommended	FileVault Additionally, Encrypted Disk Image is recommended	FileVault Additionally, Encrypted Disk Image is recommended	FileVault Additionally, Encrypted Disk Image is recommended	FileVault Additionally, Encrypted Disk Image is recommended

Better

Storage Encryption

The following software is recommended:

- **Windows XP and Windows Vista** (other than Windows Vista Ultimate) – FREE CompuSec for all security levels
- **Windows Vista Ultimate** – BitLocker for all security levels
- **Mac OS X** – File Vault for Unclassified information; Encrypted Disk Image for Confidential and Personally Identifiable Information (PII) security levels

Example 4

Awkward

TSM Configuration

Priority Class	Role Assignment
Confidentiality Low	Principal George Jetson
Integrity Medium	Custodian JIT Staff
Availability High	Users TSM Customers

TSM Logs

Priority Class	Role Assignment
Confidentiality Low	Principal George Jetson
Integrity Medium	Custodian JIT Staff
Availability Low	Users TSM Administrators

TSM Backup Data

Priority Class	Role Assignment
Confidentiality High	Principal George Jetson
Integrity High	Custodian JIT Staff
Availability High	Users TSM Customers

Better**TSM Area**

TSM information is shown in the following table. George Jetson is the principle owner of this area, and JIT staff are the custodians.

TSM Item	Priority Class			Users
	Confidentiality	Integrity	Availability	
Configuration	Low	Medium	High	TSM Customers
Logs	Low	Medium	Low	TSM Administrators
Backup data	High	High	High	TSM Customers

Example 5

Awkward

The following table describes the Communication Adapter alert codes.

Adapter name	Alert Code	Description	Action
COM/DCOM	COMCREATECOMOBECTJFAILED00 0003	Failed to create COM object instance with CLSID {0}	COM Server may not be installed. Verify whether the COM server is running. Verify that parameters are correct.
	COMNOMOREACCESSHANDLES00 0002	No more concurrent access handles available	<ul style="list-style-type: none"> Insufficient resources to run Collaboration. Consider load-balancing by deploying your Project on multiple hosts. Try re-deploying the Project. Verify that the configuration parameters are valid.
	COMUNABLETOGETCOMRUNTIME000001	Failed acquire COM runtime environment	The Runtime JNI and DLL may not be available. Verify that Runtime JNI and DLL are installed in the correct directory.
	COM -UNKNOWNAPPNAME 000004	Unrecognized application name {0}	This alert code is reserved for future enhancement.
E-mail	EMAILEWAYCHECKEMAILFAILED000004	Failed to check for available E-mail messages; host is {0}, using {1} port {2}.	Some component of the E-mail is not supported by the E-mail Adapter. E-mail message could not be parsed. Refer to the log for more information.
	EMAILEWAY-CONNECTFAILED000001	Failed to connect to host {0} on port {1} as user {2}.	<ul style="list-style-type: none"> E-mail server is not available. Verify that the E-mail server is running and that you are able to connect to the server. Parameters are not configured properly. Verify that the E-mail Adapter property values are configured correctly. Refer to the log for more information.
	EMAILEWAY-RECVFAILED000003	Failed to receive E-mail message; host is {0}, using {1} port {2}.	Parameters are not configured properly. Verify that the E-mail Adapter property values are configured correctly. Refer to the log for more information.
	EMAILEWAY-SENDFAILED000002	Failed to send E-mail message; host is {0}, using SMTP port {1}.	Parameters are not configured properly. Verify that the E-mail Adapter property values are configured correctly. Refer to the log for more information.

HTTPS	HTTPCLIENTEWAY-CONFIGFAILED000001= Configuration error encountered for HTTP Client Adapter.	Occurs if the project deployment parameters are invalid.	Connectivity Map and external configuration information is invalid. Verify configured parameters.
	HTTPCLIENTEWAY-CONNECTFAILED000002= Failed to prepare the HTTP Client agent for establishing the connection to the HTTP server.	Occurs when a socket connection does not exist.	Verify that network connectivity is available.
	HTTPCLIENTEWAY-GETFAILED000004= Failed on HTTP GET request to URL {0}.	Occurs when an HTTPS operation is not successful.	<ul style="list-style-type: none"> • Read the response code in the collaboration and proceed accordingly. • Run the operation from a web browser.
	HTTPCLIENTEWAY-POSTFAILED000005= Failed on HTTP POST request to URL {0}.	Occurs when an HTTPS operation is not successful.	<ul style="list-style-type: none"> • Read the response code in the collaboration and proceed accordingly. • Run the operation from a web browser.
	HTTPCLIENTEWAY-URLFAILED000003= Invalid URL specified {0}.	Occurs when an invalid URL is entered.	Verify that the URL is correct.

Better*Table 1: COM/DCOM Communication Adapter Alert Codes*

Alert Code	Description	Action
COMCREATECOMOBJECTJFAILED00 0003	Failed to create COM object instance with CLSID {0}	COM Server may not be installed. Verify whether the COM server is running. Verify that parameters are correct.
COMNOMOREACCESSHANDLES00 0002	No more concurrent access handles available	<ul style="list-style-type: none"> Insufficient resources to run Collaboration. Consider load-balancing by deploying your Project on multiple hosts. Verify that the configuration parameters are valid.
COMUNABLETOGETCOMRUNTIME000001	Failed to acquire COM runtime environment	The Runtime JNI and DLL may not be available. Verify that Runtime JNI and DLL are installed in the correct directory.
COM -UNKNOWNAPPNAME 000004	Unrecognized application name {0}	This alert code is reserved for future enhancement.

Table 2: Email Communication Adapter Alert Codes

Alert Code	Description	Action
EMAILWAYCHECKEMAILFAILED000004	Failed to check for available email messages; host is {0}, using {1} port {2}.	Some component of the email is not supported by the email Adapter. E-mail message could not be parsed. Refer to the log for more information.
EMAILWAY-CONNECTFAILED000001	Failed to connect to host {0} on port {1} as user {2}.	<ul style="list-style-type: none"> E-mail server is not available. Verify that the E-mail server is running and that you are able to connect to the server. Parameters are not configured properly. Verify that the E-mail Adapter property values are configured correctly. Refer to the log for more information.
EMAILWAY-RECVFAILED000003	Failed to receive E-mail message; host is {0}, using {1} port {2}.	Parameters are not configured properly. Verify that the E-mail Adapter property values are configured correctly. Refer to the log for more information.
EMAILWAY-SENDFALLED000002	Failed to send E-mail message; host is {0}, using SMTP port {1}.	Parameters are not configured properly. Verify that the E-mail Adapter property values are configured correctly. Refer to the log for more information.

Table 3: HTTPS Communication Adapter Alert Codes

Alert Code	Description	Action
HTTPCLIENTEWAY-CONFIGFAILED000001= Configuration error encountered for HTTP Client Adapter	Occurs if the project deployment parameters are invalid	Connectivity Map and external configuration information is invalid. Verify configured parameters.
HTTPCLIENTEWAY-CONNECTFAILED000002= Failed to prepare the HTTP Client agent for establishing the connection to the HTTP server	Occurs when a socket connection does not exist	Verify that network connectivity is available.
HTTPCLIENTEWAY-GETFAILED000004= Failed on HTTP GET request to URL {0}	Occurs when an HTTPS operation is not successful	<ul style="list-style-type: none"> • Read the response code in the collaboration and proceed accordingly. • Run the operation from a web browser.
HTTPCLIENTEWAY-POSTFAILED000005= Failed on HTTP POST request to URL {0}	Occurs when an HTTPS operation is not successful	<ul style="list-style-type: none"> • Read the response code in the collaboration and proceed accordingly. • Run the operation from a web browser.
HTTPCLIENTEWAY-URLFAILED000003= Invalid URL specified {0}	Occurs when an invalid URL is entered	Verify that the URL is correct.

FAQ Guidelines

Example 1

Awkward

Where do I find my local system administrator?

Jetson Industries is running its support on a centralized service model. This is based on Regional Service Centers (RSCs). These are responsible for providing IT infrastructure support for a given region (i.e. Countries). Engineer are dispatched from these RSCs for solving major emergencies (like site downs) which cannot be solved remotely. For normal operation support IT Ops partners with suppliers like Enterprise Services, AGM, Johnson Control, Lexmark, Xerox and others. On top of these some local Jetson employees like ES engineers, sales engineers offer their help to debug tricky problems at remote sites together with IT Ops. I want to hereby express my sincerest thanks to all the Jetsonites who help IT Operations on a voluntary basis. On top of that most of the direct user support is done via HelpDesk and the three Resolution Centers (RCs) around the globe.

Better

Who is my local system administrator and how do I contact that person?

For IT support, call the Resolution Center at x12345 or file a HelpDesk request at <http://jetsonweb.region/helpdesk/>.

Example 2

Awkward

BugTag FAQ: Notes

1. How can I delete a Note?
2. How can I see the existing Comments notes while I am adding a new Comments note?
3. What are the navigation controls for notes?
4. Why are text fields sometimes greyed out?
5. Should I add a new entry to a note or modify an existing one?
6. How do I edit existing notes in release 2.2?
7. What are viewing modes?
8. How do I add notes in release 2.2?
9. Why were multiple note entries implemented in release 2.2?
10. What are Floating Notes and how does it work?
11. What are the keyboard shortcuts for undo and redo on notes?
12. What if I don't see a time stamp in the Notes?
13. Is there a way to search for a particular 'keyword' in the Engineering Notes?
14. What are the different Note types in the Notes table?
15. How long can a note be?
16. Is the Description field private?
17. Will the user be notified if a note larger than 16K is posted?
18. Where are Work Arounds located?
19. Are all engineering notes made public?
20. How many users had notes more than 16k in BugTag?
21. Who can change Note entries?
22. Can a user append to existing text in the Comment/ Description/Work Around Note types?

Better

Notes

For detailed information about how to use the Notes feature of BugTag 2.2, see the documentation at <http://jetsonweb.corp/bugtag/docs/>.

This FAQ answers some common troubleshooting questions.

- Why are text fields sometimes greyed out?
- Why do some notes not display a time stamp?
- Is it safe to put private information in the Description?
- Can I search for a keyword in the Engineering notes?
- Where are workarounds located?

Example 3

Awkward

VDT FAQ

Very often, a list of so-called Frequently Asked Questions is simply an excuse not to write decent documentation. If you find problems with our documentation, please [let us know](#) and we will try to fix the documentation to meet your needs.

That said, there are some commonly asked questions that don't fit elsewhere, so we will answer them here.

1. Why should I use the VDT instead of getting software directly from the people that make it?

1. Much of the software provided by the VDT is complex to install and configure. The VDT installation process hopefully makes this much easier for you.

2. We patch some of the software with the latest bug fixes that are hard to track down and apply yourself.

3. We provide a complete package so you don't have to get software from many locations

2. How do I download the VDT?

Normally you don't, but you use Pacman--an installation program--to do so. If you wish you can download RPMs and Debian packages for a subset of the VDT.

[More information...](#)

3. Why do you use Pacman instead of RPM, Debian packages, or <Your favorite packaging format>?

Pacman can run as root or non-root. Pacman is easy for non-system administrators to use. Pacman is a convenient solution when software packages are delivered to us in many formats. And we are planning on supplying a more complete set of RPMs and Debian packages in the future so you can choose what you prefer.

[More information...](#)

Better

VDT FAQ

This FAQ answers the most frequently asked questions about the Virtual Data Toolkit (VDT) from our users. Please consult the [product documentation](#) for details about using the VDT. If you have any questions about the documentation or the product, [contact us](#).

Why should I use VDT instead of getting software directly from the source?

Using VDT provides the following advantages:

- The VDT installation process means that you don't have to deal with each product's individual installation and configuration processes, which are often complex.
- You don't have to access the location of each separate software product.
- The VDT provides automatic patches of the software with the latest bug fixes, so you don't have to monitor them, find them, and install them yourself.

How do I download the VDT?

If you use the provided installation program, Pacman, you don't have to download the VDT at all. If you prefer, you can download individual RPMs and Debian packages to install a subset of the VDT, as described in the [VDT documentation](#). We plan to supply a more complete set of RPMs and Debian packages in the future. However, these packages don't include various VDT configuration utilities.

Why do you use Pacman instead of other packaging formats?

Pacman provides the following advantages:

- Can run as root or non-root
- Is easy for non-system administrators to use
- Provides a consistent installation interface rather than the different formats in which the individual software packages are delivered

Illustration Guidelines

Example 1

Awkward

See the sample file thunderbird-spamfilter.html.

Better

See the sample file new-thunderbird-spamfilter.html.

Example 2

Awkward

The following tape volume pools have been created to cater for the segregation of media into the categories:

Volume Pool	Number	User	Host	Group	Description	Scratch
DataStore	2	root(0)	ANYHOST	NONE	the DataStore pool	No
NetBackup	1	root(0)	ANYHOST	NONE	the NetBackup pool	No
None	0	ANY	ANYHOST	NONE	the None pool (for anyone)	No
SCRATCH	7	ANY	ANYHOST	NONE	All scratch tapes	Yes
unix-daily	3	ANY	ANYHOST	NONE	Daily Backup tapes (unix)	No
unix-monthly	5	ANY	ANYHOST	NONE	Monthly Backup tapes (unix)	No
unix-weekly	4	ANY	ANYHOST	NONE	Weekly Backup tapes (unix)	No
unix-yearly	6	ANY	ANYHOST	NONE	Yearly Backup tapes (unix)	No
windows-daily	8	ANY	ANYHOST	NONE	Daily Backup tapes (win)	No
windows-monthly	10	ANY	ANYHOST	NONE	Monthly Backup tapes (win)	No
windows-weekly	9	ANY	ANYHOST	NONE	Weekly Backup tapes (win)	No
windows-yearly	11	ANY	ANYHOST	NONE	Yearly Backup tapes (win)	No

Better

The tape volume pools for nb-mitch1 listed in the following table segregate the media into categories.

Volume Pool	Number	User	Host	Group	Description	Scratch
DataStore	2	root(0)	ANYHOST	NONE	DataStore pool	No
NetBackup	1	root(0)	ANYHOST	NONE	NetBackup pool	No
None	0	ANY	ANYHOST	NONE	None pool (for anyone	No
SCRATCH	7	ANY	ANYHOST	NONE	All scratch tapes	Yes
unix-daily	3	ANY	ANYHOST	NONE	Daily backup tapes (UNIX)	No
unix-monthly	5	ANY	ANYHOST	NONE	Monthly backup tapes (UNIX)	No
unix-weekly	4	ANY	ANYHOST	NONE	Weekly backup tapes (UNIX)	No
unix-yearly	8	ANY	ANYHOST	NONE	Yearly backup tapes (UNIX)	No
windows-daily	8	ANY	ANYHOST	NONE	Daily backup tapes (Windows)	No
windows-monthly	10	ANY	ANYHOST	NONE	Monthly backup tapes (Windows)	No
windows-weekly	9	ANY	ANYHOST	NONE	Weekly backup tapes (Windows)	No
windows-yearly	11	ANY	ANYHOST	NONE	Yearly backup tapes (Windows)	No